# 準パススルー型 VMM のマルウェア検出機能による拡張

Tran Truong Duc Giang † 大山恵弘 †

## 1. はじめに

近年，コンピュータの利用における情報漏洩の被害が拡大している．情報漏洩の原因の一つは悪意のプログラム (マルウェア) である．情報漏洩を防止するために，OS にアンチマルウェアを導入することが一般的となっている．この方法は効果的であるが，いくつかの問題がある．特に深刻な問題は，マルウェアによる OS の改竄や，ユーザの故意またはミスに起因する操作により，アンチマルウェア機能が無効化される可能性があるというものである．その問題に対処するために，OS から分離された仮想マシンモニタ (VMM) にセキュリティ機能を配置するアプローチが注目されている．本研究では，セキュリティ向上を目的としている仮想マシンモニタ BitVisor[1] 内でマルウェア検出機能を実現する．仮想マシンモニタ内で実現することにより，上記の問題の解決に加えて，特定の OS に依存しない形でマルウェア検出が行えるという利点が得られる．

## 2. BitVisor の概要

BitVisor とは，筑波大学などによって開発された，ハードウェア上で直接動作する軽量な仮想マシンモニタである．BitVisor は，準パススルー型と呼ばれる方式を利用する．準パススルー型とは，ゲスト OS からハードウェアに可能な限り透過的にアクセスさせ，セキュリティ機能の実現のために，最低限必要なアクセスのみを仮想マシンモニタで捕捉する方式である．一部のアクセスのみを捕捉することにより，ストレージやネットワークの暗号化などのセキュリティ機能を実現することができる．

図 1 に示すように，仮想マシンモニタで捕捉する必要があるアクセスには，制御 I/O とデータ I/O の 2 種類がある．制御 I/O は，デバイスによるデータ転送を制御するための I/O で，転送するデータの場所やアクセス方法，データ転送の開始，終了などを指定する．データ I/O は，実際にデータ転送を行う I/O である．仮想マシンモニタが制御 I/O を捕捉してアクセスの状態を把握し，データ I/O を捕捉してデータを取得，更新することにより，ゲスト OS から透過的に暗号化/復号化の処理を実現できる．

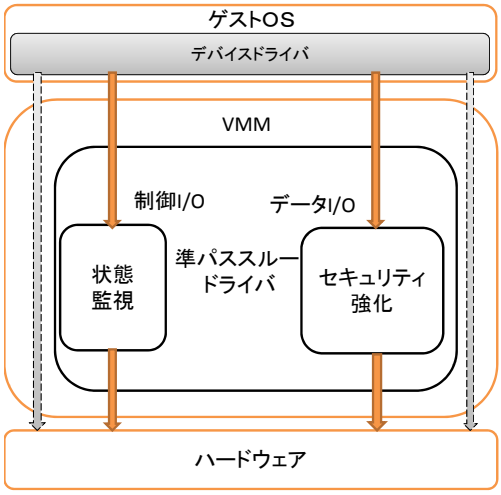


**図 1** 準パススルー型 VMM の構成

## 3. 設計方針

本研究のシステムでは，図 2 のように，ATA デバイス，ネットワークデバイス，USB ストレージデバイスによるデータ I/O の内容をマルウェアのシグネチャとマッチングすることによりマルウェアを検出する．以下では，ATA デバイスが扱う I/O データに対するシグネチャマッチングの設計を述べる．

準パススルー型 VMM は，ホスト OS を持たないため，シグネチャデータをホスト OS のファイルシステムに置くことはできない．そこで，BitVisor のメモリ領域にシグネチャデータを予め埋め込んでおくものとする．本研究のシステムは，マルウェアのシグネチャデータとして ClamAV[2] が提供するシグネチャ定義データを利用する．

BitVisor では，PIO(プログラム I/O)，メモリマップド I/O，DMA(Direct Memory Access) の 3 つの

† 電気通信大学大学院電気通信学研究科情報工学専攻

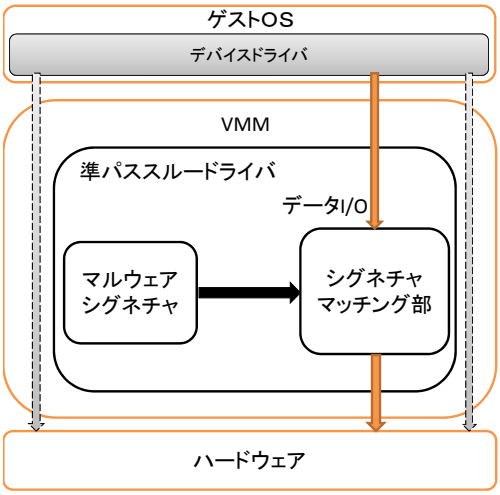


**図 2** シグネチャマッチングの仕組み

転送方式によるデータ I/O アクセスが捕捉できる．本研究のシステムは，それらすべての方式による I/O データに対してシグネチャマッチングを行う．

BitVisor は，データ I/O の値が実際にストレージに読み書きされる前に暗号化を行い，ストレージから読み出された後に復号化を行う．暗号化される前の時点で，仮想マシンモニタのバッファに溜まるデータに対してシグネチャマッチングを行う．シグネチャに該当するバイト列がある場合，そのバイト列を別のバイト列に置換したり，アクセスを失敗させるなどの対策処理を実行する．

## 4. 現状と今後の予定

現状では，ATA デバイスの I/O データに対するシグネチャマッチング機構を実装中である．ATA デバイスに対する実装が完了したら，順にネットワークデバイスと USB ストレージデバイスの I/O データに対するシグネチャマッチングの実装を行う．

## 謝　　辞

本研究の一部は総務省戦略的情報通信研究開発推進制度 (SCOPE) の支援を受けて行われた．

## 参 考 文 献

1) Takahiro Shinagawa, Hideki Eiraku, et al., BitVisor: A Thin Hypervisor for Enforcing I/O Device Security; *In Proceedings of the 2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments; pp. 121-130, March 2009.*
2) ClamAV, http://www.clamav.net/